document management, correspondence and action tracking, configuration management, and text search but appear to be duplicating efforts in a non-standard fashion.

- There is little support for open systems standardized approaches to automated interchange of complex mixed-mode documents and data sets beyond text and some GIS interchanges. Text is largely interchanged through word processor formats and not open systems approaches such as Standard Generalized Markup Language (SGML) and more recently Extensible Markup Language (XML). XML is an application of SGML intended to replace Hypertext Markup Language (HTML) on the Web.

- Currently, within FEMA, there is perhaps an over-reliance on declaring tools, even if proprietary, to be the FEMA IT enterprise standard, as opposed to defining standard approaches to document and data interchange.

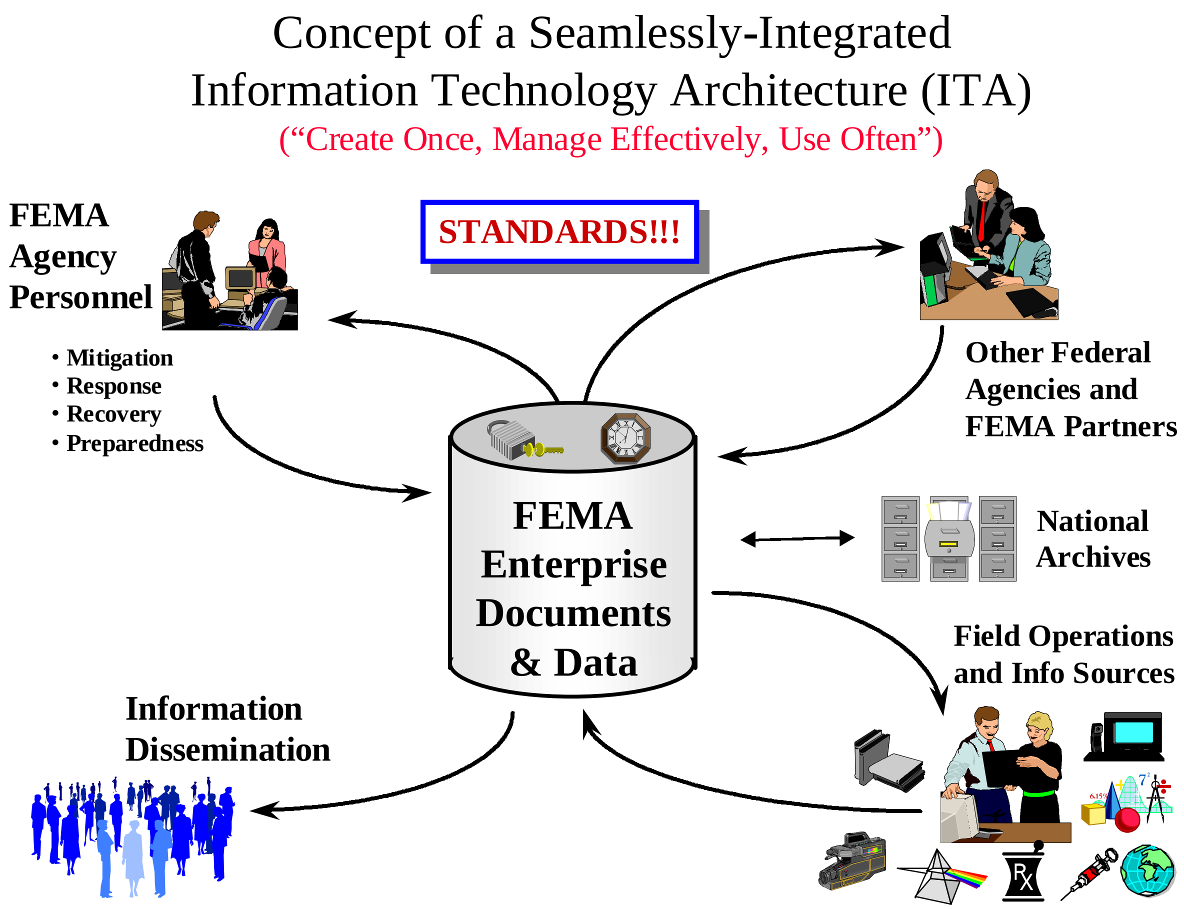
- Electronic records, documents, and data in FEMA IT systems and databases are not locked through secure digital signatures, date-time stamping, and secure hash mechanisms. While not a high priority concern and while other security mechanisms are in place, it would be somewhat problematic for FEMA to verify unequivocally in a court of law that formal electronic documents and data sets have not been altered. FEMA understands that this is common problem for many other Federal agencies, and data protection and integrity issues are widely recognized to be a concern for the CIP program.

1.10 FEMA Target IT Architecture and Requirements for Enhanced Automation

This section of the *FEMA IT Architecture* provides the target vision and requirements for enhanced automation. FEMA and its enterprise partners share a common set of goals and objectives with regard to emergency planning and operations, including the four major phases of CEM, i.e., Mitigation, Preparedness, Response, and Recovery. In an enterprise-sense, FEMA wishes to exploit information technology consistent with the evolving National and Global Information Infrastructure (NII/GII) and ongoing efforts to develop Digital Government as articulated by the National Performance Review. These principles are congruent with the ITMRA, which requires that Federal agencies produce IT architectures to guide their resource allocation decisions.

FEMA, in cooperation with its enterprise partners, wishes to develop and implement capabilities for secure and intelligent, bi-directional, electronic document and data interchange in a widely-distributed collaborative environment. Consistent with the requirements of public law and national-level directives, the model for creating, managing, and using such electronic documents and data must work in a legal and regulatory framework.

As shown in Figure 1-3, FEMA and its enterprise partners share common problems associated with distributed collaboration on, and interchange and representation of, complex information (including text, graphics, and multimedia objects; and engineering, GIS, mathematical, radiological, human services, medical, chemical and environmental, weather, geologic, and transportation data) in an intelligent and searchable electronic format. This concept is the essence of *creating documents and data sets once in their most intelligent form, effectively managing them throughout their life cycle, and deriving maximum downstream re-use of the information*.



Concept of a Seamlessly-Integrated
Information Technology Architecture (ITA)
("Create Once, Manage Effectively, Use Often")

STANDARDS!!!
FEMA Agency Personnel
• Mitigation
• Response
• Recovery
• Preparedness
Other Federal Agencies and FEMA Partners
FEMA Enterprise Documents & Data
National Archives
Field Operations and Info Sources
Information Dissemination

Figure 1-3. FEMA Enterprise Architectural Concept of Creating, Managing, and Using Documents and Data in an Intelligent Format

FEMA has vital concerns about how electronic objects can stand up to data integrity and security management requirements in an electronic environment that is widely distributed in a telecommunications sense and exploits video teleconferencing and other high bandwidth collaborative technology. It is reasonable to believe that FEMA's enterprise partners share these concerns. With recent court cases, FEMA is also aware that it is no longer adequate to assume that printed copies of the records will be legally acceptable in a court of law in *lieu* of the electronic records. Accordingly, the *FEMA IT Architecture* adopts a strong standards-based approach toward future development and implementation. Widely implemented, internationally-accepted, open systems standards for the representation, interchange, collaboration, and visualization of documents and data in an intelligent electronic format are recognized as a problem at all levels of government, and throughout industry.

Integration of IT Systems and Processes into the Network Architecture. As illustrated in Figure 1-4, for FEMA integration of IT technology to create data once in its most intelligent form, manage it across its life cycle, and then gain maximum re-use (mitigation activities being an excellent example), IT systems demand a robust, distributed networking and communications environment. Within FEMA, IT systems must be seamlessly integrated with the network environment. Section 3 of this *FEMA IT Architecture* identifies the target network architecture in more detail. Figure 1-4 further identifies some of the anticipated benefits in achieving this level of integration.

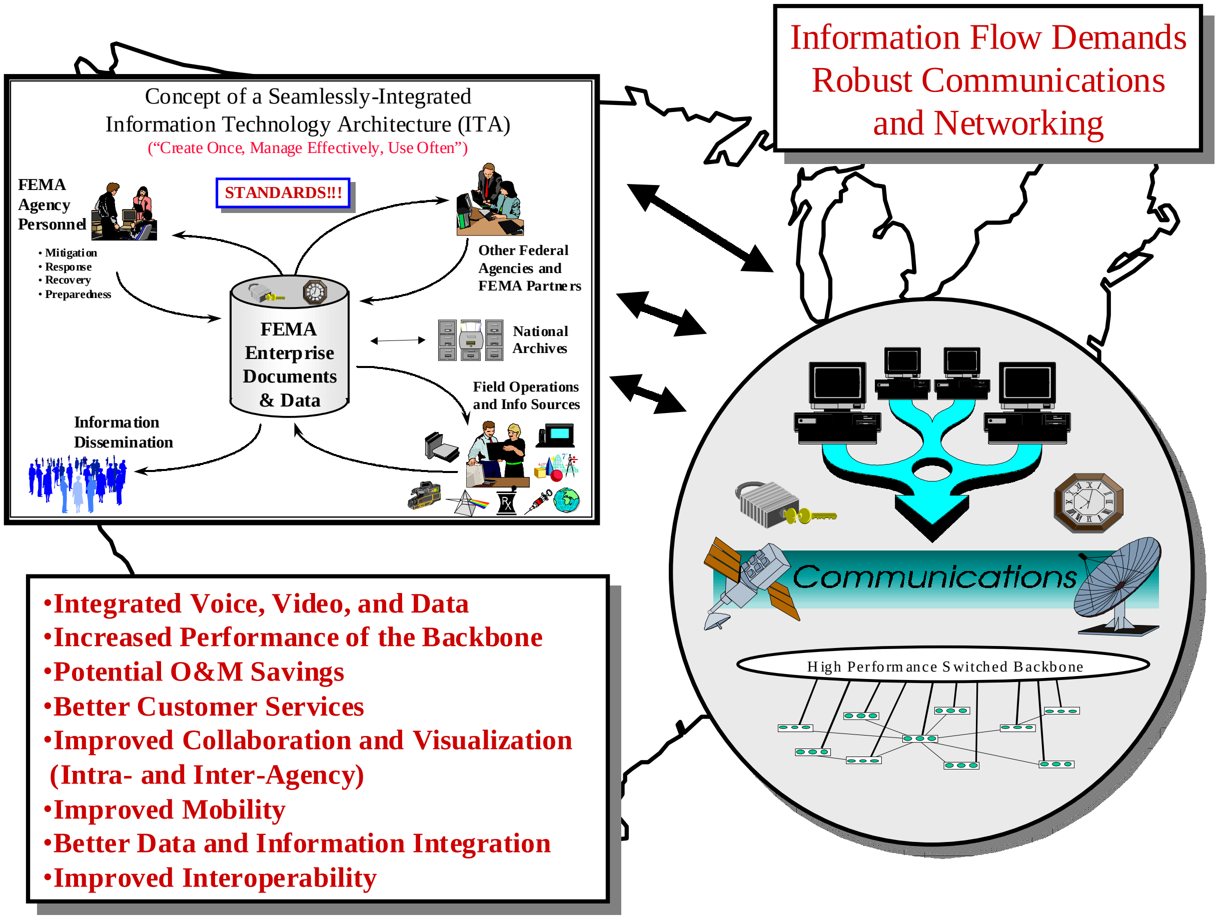

Information Flow Demands
Robust Communications
and Networking
Concept of a Seamlessly-Integrated
Information Technology Architecture (ITA)
("Create Once, Manage Effectively, Use Often")
FEMA Agency Personnel
• Mitigation
• Response
• Recovery
• Preparedness
STANDARDS!!!
Other Federal Agencies and FEMA Partners
FEMA Enterprise Documents & Data
National Archives
Field Operations and Info Sources
Information Dissemination
Communications
High Performance Switched Backbone
•Integrated Voice, Video, and Data
•Increased Performance of the Backbone
•Potential O&M Savings
•Better Customer Services
•Improved Collaboration and Visualization
(Intra- and Inter-Agency)
•Improved Mobility
•Better Data and Information Integration
•Improved Interoperability

Figure 1-4. Integration of IT Systems Environment into the Networking Environment

Target Architecture Vision. Figure 1-5 depicts an overall architectural vision for FEMA that seamlessly integrates IT systems, data, and architectural components in a robust networking and communications environment. The fundamental goal of the target architecture is to support the notion of *Comprehensive Emergency Management* in the areas of mitigation, preparedness, response, and recovery as articulated in the *FEMA Strategic Plan*. In reference to Figure 1-5, the target *FEMA IT Architecture* has the following major characteristics.

- **Well-Integrated Enterprise-Wide Systems and Services.** Currently, there is considerable ongoing effort to develop and integrate a number of distributed enterprise-wide IT systems. In the target architecture, FEMA enterprise-wide systems will be well-integrated and interoperable to the extent required by the design requirements as approved by the CIO in consultation with the IRB. This means that the systems support the concept of *Create Once, Manage Effectively, and Use Often* in a seamless and secure manner. In the target architecture, all FEMA enterprise systems are considered mission-critical and must meet the stated operational environmental factors for the functions that they support. They shall be designed, developed, tested, and integrated in accordance with the *FEMA IT Architecture*. They shall also be developed, maintained, and operated to afford critical infrastructure protection and assurance consistent with EO 13010 and PDD-63. In the system development and integration process, it is anticipated that FEMA enterprise systems will assume the lead role in developing standardized services and capabilities (i.e., common reusable architectural components) that will be made broadly available to other clients such as standalone program-centric systems and users across the enterprise. In this regard, FEMA recognizes that its $70M investment in the NEMIS infrastructure and environment presents significant opportunities for FEMA to integrate other currently isolated and standalone areas of FEMA information systems. In the development of the *FEMA IT Architecture*, the **NEMIS project is the lead development and integration project for defining and implementing a *FEMA IT Architecture* baseline**. In implementation of the *IT Architecture*, the ITS Directorate is open to innovation and good ideas from other organizational elements and enterprise systems.

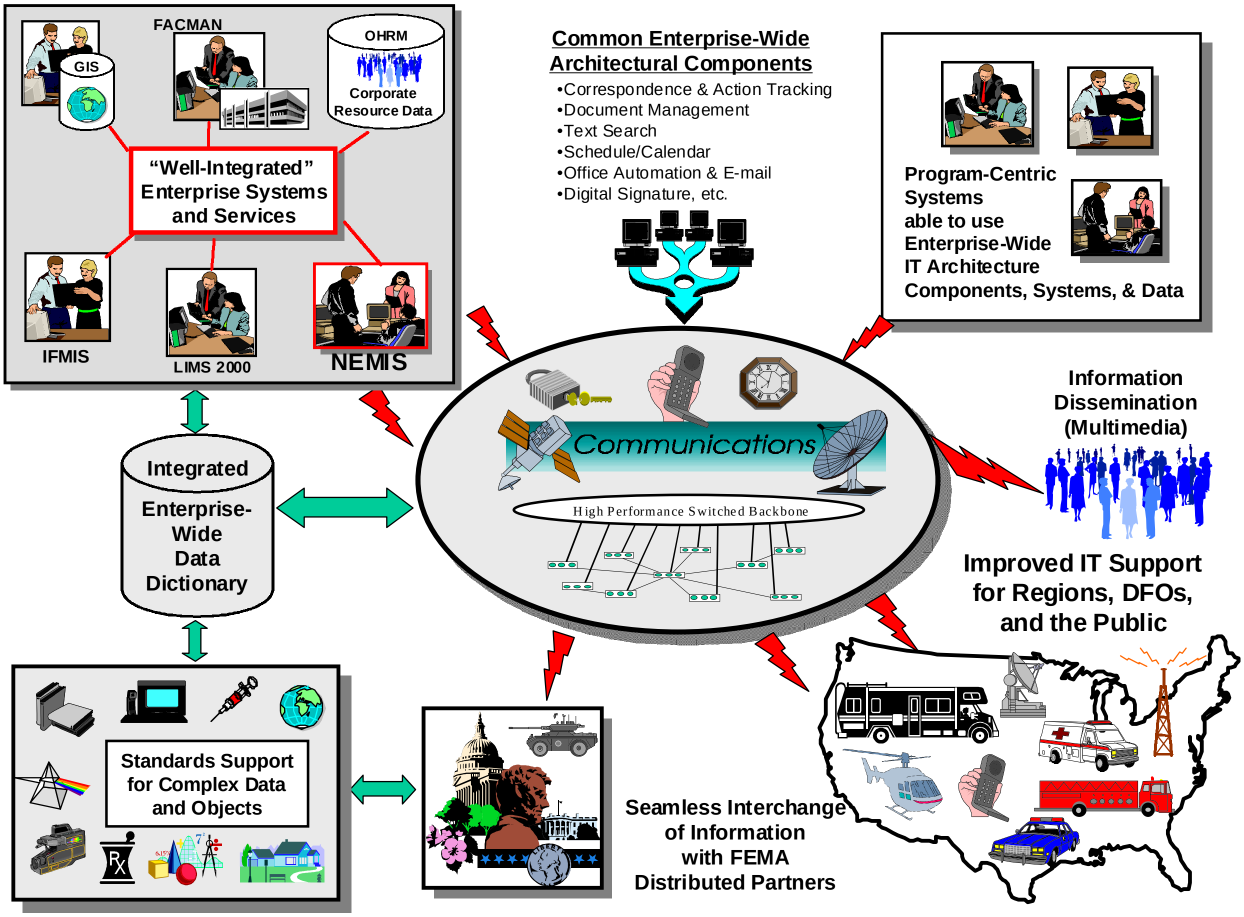

FACMAN
OHRM
GIS
Corporate Resource Data
"Well-Integrated" Enterprise Systems and Services
IFMIS
LIMS 2000
NEMIS
Common Enterprise-Wide Architectural Components
•Correspondence & Action Tracking
•Document Management
•Text Search
•Schedule/Calendar
•Office Automation & E-mail
•Digital Signature, etc.
Program-Centric Systems able to use Enterprise-Wide IT Architecture Components, Systems, & Data
Communications
High Performance Switched Backbone
Information Dissemination (Multimedia)
Integrated Enterprise-Wide Data Dictionary
Improved IT Support for Regions, DFOs, and the Public
Standards Support for Complex Data and Objects
Seamless Interchange of Information with FEMA Distributed Partners

Figure 1-5. ***FEMA IT Architecture*** **Target Vision**

As shown in Figure 1-5, FEMA enterprise-wide IT systems include:

- National Emergency Management Information System (NEMIS), which is operational in its Version 1 release. The FEMA ITS Directorate will conduct a series of Joint Application Development (JAD) sessions across FEMA in an initial effort to baseline future NEMIS Version 2 requirements. Depending on funding, potential candidates for future enterprise-wide functionality to be incorporated in NEMIS Version 2 include:
  - A FEMA Grants Management capability
  - An Exercise and Training Module integrated with response and recovery functionality to simulate emergencies in a virtual environment and to support distributed exercise planning, operations, reconstruction, and analysis

    - Improved interfaces and/or some reallocation of functionality with other enterprise systems (e.g., LIMS, IFMIS, FACMAN, GIS, and OHRM's CRD)
    - Improved enterprise-wide functionality in such areas as digital libraries, security and information assurance, data warehousing, workflow management, text search, document management, digital signatures, and correspondence and action tracking.
  - The Integrated Financial Management Information System (IFMIS)
  - The Logistics Information Management System (LIMS) 2000
  - The Facilities Management (FACMAN) system
  - The FEMA Geographic Information System (GIS), with support from the Map Service Center (MSC) and the Map Analysis Center (MAC). The current GIS capability is somewhat fragmented across FEMA. An enterprise-wide, integrated capability is needed.
  - Office of Human Resources Management's Corporate Resource Data Base (CRD) supported by various information systems and servers.

- **Improved Communications and Networking**. In the target architecture, communications and networking will be supported by an integrated high-performance switched backbone. Section 3 of this *FEMA IT Architecture* describes the target network architecture in more detail. Depending on funding, the target network architecture may evolve to support integrated voice, video, and data applications and higher bandwidth applications, including streaming multimedia to the public for information dissemination purposes as well as distributed interactive simulations for exercises. Core capabilities may be provided through the implementation of Asynchronous Transfer Mode (ATM) technology. In the target architecture, increased emphasis may be placed on Personal Communications System (PCS) technology and Global Positioning System (GPS) for operations in the field. Increased emphasis will also be placed on CIP aspects of the FEMA network architecture.

- **Consideration for Legacy Telecommunications Systems as New Capability Is Added.** Important legacy telecommunications systems such as HF radio and the National Warning System (NAWAS) will be preserved for the time being to meet continuing critical operational requirements. The goal is to have a network environment that meets all of the operational requirements, operates better, and costs less across the spectrum of emergencies. In the target architecture, benefits can be expected at all operational levels as illustrated in Figure 1-6.

- **Bandwidth Less of a Concern for Advanced IT Applications.** In the future network architecture, bandwidth limitation will be less of a factor and the network will be designed to provide adaptive Quality of Service (QoS). This approach and philosophy is consistent with the Next Generation Internet (NGI) and Internet2 projects. Depending on funding, the proposed target network architecture will be scaleable and will support bandwidth-intensive and potentially-demanding IT applications such as:
  - Multimedia applications and graphics-intense interchange
  - Public information dissemination of multimedia objects such as streaming audio and video
  - Data-intense GIS applications
  - Intelligent distributed collaboration and visualization applications
  - Integrated voice, video, and data applications
  - Future digital library applications where an enterprise-wide document management or text search capability might be incorporated
  - Distributed interactive simulations for exercise support
  - Future virtual reality applications such as 3-D simulations for fire-fighting or telepresence purposes.

Figure 1-6 depicts the relative requirements for bandwidth for various IT architectural components that have been identified. The figure also depicts the relative requirements for the transmission of data across the network to be *steady* as opposed to *bursty* in nature.

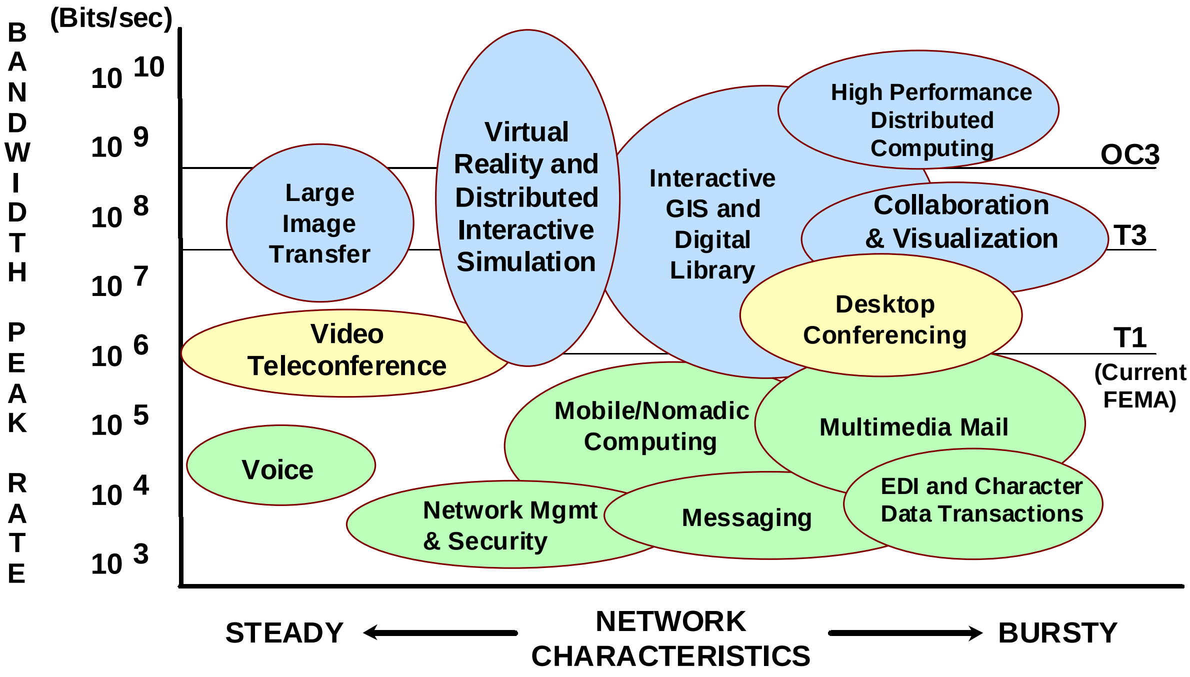


Figure 1-6. Bandwidth Requirements and Network Characteristics for Various Advanced Information Technologies

- **Potential for Increased Connectivity.** As noted above, the current FEMA network architecture is largely centralized in its national operations and management (O&M). With security concerns such as firewalls properly considered, and policies and procedures properly implemented, the target network architecture provides opportunities to potentially establish Extranets, gateways, and Virtual Private Networks (VPNs). Opportunities should be explored with the Regions to establish connectivity with FEMA's enterprise partners and with State/local governments. This should result in improved performance and information interchanges in an automated fashion.

- **Responsiveness to Consensus on Standards.** FEMA hopes that the target *FEMA IT Architecture*, with its Technical Reference Model (TRM), will help to bring consensus among the Agency's business partners on standards to support the interchange of electronic documents, data, and complex objects in a seamless and more intelligent fashion. The goal will be to employ the concept of *"Create Once, Manage Effectively, and Use Often"* and to minimize the need for scanning and re-keying of data. FEMA will be attentive to a consensus that emerges. Within its limited resources, FEMA, including its Regions, may engage with its business partners in prototyping and piloting components of the new IT and NT architectures.

- **Engineering Concerns Addressed.** In the target architecture, a number of ancillary issues lingering from the current architecture will be addressed and resolved. These include:

- Configuration management of systems, networks, data, and metadata shall be consistently performed and shall employ a standardized enterprise-wide approach.
- Data dictionaries for enterprise-wide systems and standalone, program-centric systems shall be standardized and harmonized to achieve semantic and syntactic data integrity across the enterprise.
- In development of IT systems, there will be increased emphasis on employing standardized life-cycle models. This might include increased emphasis on employing processes and procedures from the Software Engineering Institute (SEI).
- A number of standalone or program-centric information systems and data bases are expected to be consolidated and/or retired. Standalone systems and program-centric systems will continue to be permitted, though they will be mandated to employ common enterprise-wide architectural components if they need such services. Common architectural services are identified below.
- Consistent with the architectural principles stated in Appendix H , there will be increased and improved support for open systems standardized approaches to automated interchange of complex mixed-mode documents, objects, and data sets beyond current free-form unstructured text and GIS data.
- Increased emphasis will be placed on IT systems security engineering to meet the goals and objectives of the Critical Infrastructure Protection (CIP) program.

- **Tools and Open Systems Standards.** Due to its inability to affect the design of IT products, FEMA will continue its general practice of declaring tools to be FEMA IT enterprise standards. Where it appears practical to do so, FEMA will specify open system standards.

- **Improved Data Integrity over the Life Cycle.** Consistent with the direction of the CIP program, electronic records, documents, and data in FEMA IT systems and data bases will have increased levels of assured data integrity. With adequate policies and procedures in place, the architecture will evolve to support secure digital signatures, date-time stamping, long-term archival access, and secure hash mechanisms. FEMA will respond promptly to initiatives of other Federal agencies to help address this common problem.

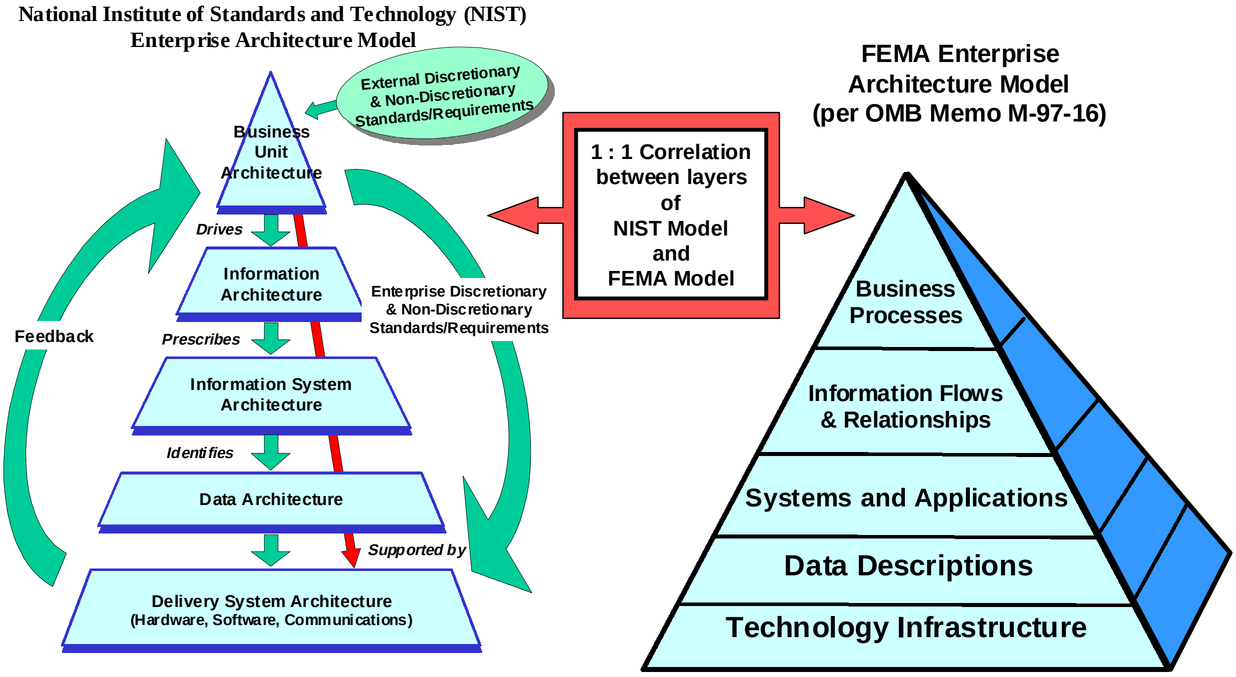
Identification of Common Architectural Components. In preparing this initial *FEMA IT Architecture*, the ITS Directorate conducted a series of interviews with senior managers, analysts, and engineers across the organization, including the Regions. The respondents identified a common set of IT needs that can be met through an approach of standardization across the enterprise. In general, the respondents warmly embraced the concept of a common enterprise approach to addressing common IT needs, as opposed to *going it alone*. The following list presents the IT architectural needs that were expressed most often.

1. Digital library services for creating, managing, and using complex mixed-mode documents and data sets including enterprise-wide search and retrieval services and data warehousing
2. Enterprise-wide data dictionary standardization
3. Correspondence and action tracking services
4. Grant management system services
5. Increased access to, and integration of, GIS products and services
6. Better office automation products
7. Improved ability for collaboration and visualization of documents and data sets (especially GIS data sets) in a distributed environment
8. Improved support for distance learning activities
9. Access to an enterprise-wide document management system

10. Support for digital notaries and digital signature services
11. Improved electronic capture and support of legacy documents and paper
12. Improved utilization of the Internet for high-volume information dissemination and for collaborative and planing activities
13. Improved support for secure electronic commerce and electronic data interchange (EDI)
14. Enterprise support for multimedia integration, including streaming audio and video
15. Improved document and data support for mobile users
16. More direct connectivity to FEMA's business partners and the States through Extranets and Virtual Private Networks
17. Adoption of standardized tools in such areas as configuration management and systems engineering.

1.11 Mapping of FEMA Target IT Architecture to the NIST Model

As illustrated in Figure 1-7, the *FEMA IT Architecture* model is patterned after and correlates well to the National Institute of Standards and Technology (NIST) Enterprise Architecture, which is documented in NIST Special Publication 500-167, entitled *Information Management Directions: The Integration Challenge.*


National Institute of Standards and Technology (NIST)
Enterprise Architecture Model
External Discretionary & Non-Discretionary Standards/Requirements
Business Unit Architecture
Drives
Information Architecture
Enterprise Discretionary & Non-Discretionary Standards/Requirements
Prescribes
Feedback
Information System Architecture
Identifies
Data Architecture
Supported by
Delivery System Architecture
(Hardware, Software, Communications)
1 : 1 Correlation between layers of NIST Model and FEMA Model
FEMA Enterprise Architecture Model (per OMB Memo M-97-16)
Business Processes
Information Flows & Relationships
Systems and Applications
Data Descriptions
Technology Infrastructure

Reference: NIST Special Publication 500-167,
"Information Management Directions: The Integration Challenge"

Figure 1-7. Mapping of Target *FEMA IT Architecture* to the NIST Model

As indicated in OMB guidance, the NIST model has been widely promoted in the Federal government as a management tool to illustrate the interconnectivity of the business, information, systems, data, and network technology environments of an enterprise and their relationships. The NIST model provides a five-tiered framework for building an integrated set of information and information technology architectures. As illustrated, the five tiers are defined separately but are

Page Down